Suricata Update Documentation

Release 1.3.2

OISF

Mar 14, 2024

CONTENTS

1 Quick Start **1**
- 1.1 Install Suricata Update . . . 1
- 1.2 Directories and Permissions . . . 2
- 1.3 Update Your Rules . . . 3
- 1.4 Configure Suricata to Load Suricata-Update Managed Rules . . . 3
- 1.5 Discover Other Available Rule Sources . . . 4
- 1.6 List Enabled Sources . . . 4
- 1.7 Disable a Source . . . 4
- 1.8 Remove a Source . . . 4

2 suricata-update - Update **5**
- 2.1 Synopsis . . . 5
- 2.2 Description . . . 5
- 2.3 Options . . . 5
- 2.4 Rule Matching . . . 8
- 2.5 Order of application of configuration files . . . 10
- 2.6 Example Configuration Files . . . 10

3 update-sources - Update the source index **15**
- 3.1 Synopsis . . . 15
- 3.2 Description . . . 15
- 3.3 Options . . . 15
- 3.4 Files and Directories . . . 16
- 3.5 Environment Variables . . . 16
- 3.6 URLs . . . 16

4 list-sources - List available sources **17**
- 4.1 Synopsis . . . 17
- 4.2 Description . . . 17
- 4.3 Options . . . 17

5 enable-source - Enable a source **19**
- 5.1 Synopsis . . . 19
- 5.2 Description . . . 19
- 5.3 Options . . . 19

6 disable-source - Disable an enabled source **21**
- 6.1 Synopsis . . . 21
- 6.2 Description . . . 21
- 6.3 Options . . . 21

7 remove-source - Remove a configured source **23**
7.1 Synopsis . . . 23
7.2 Description . . . 23
7.3 Options . . . 23

8 add-source - Add a source by URL **25**
8.1 Synopsis . . . 25
8.2 Description . . . 25
8.3 Options . . . 25
8.4 Common Options . . . 26

9 check-versions - Check version of Suricata **27**
9.1 Synopsis . . . 27
9.2 Description . . . 27
9.3 Options . . . 27

Index **29**

CHAPTER

ONE

QUICK START

1.1 Install Suricata Update

Suricata-Update is bundled with all supported versions of Suricata and should be installed when Suricata is installed. Please check if `suricata-update` is already installed before proceeding with these installation directions, for example, the following command will tell you the version:

```
suricata-update -V
```

You should only need to install Suricata-Update manually if it is required independently of a Suricata install.

Suricata-Update is a tool written in Python and best installed with the `pip` tool for installing Python packages.

Pip can install `suricata-update` globally making it available to all users or it can install `suricata-update` into your home directory.

To install `suricata-update` globally:

```
pip install --upgrade suricata-update
```

or to install it to your own directory:

```
pip install --user --upgrade suricata-update
```

Pip can also be used to install the latest development version of Suricata-Update:

```
pip install --user --upgrade \
    https://github.com/oisf/suricata-update/archive/master.zip
```

Note: When installing to your home directory the `suricata-update` program will be installed to $HOME/.local/bin, so make sure this directory is in your path:

```
export PATH=$HOME/.local/bin:$PATH
```

1.2 Directories and Permissions

In order for `suricata-update` to function, the following permissions are required:

- Directory /etc/suricata: read/write access
- Directory /var/lib/suricata/rules: read/write access
- Directory /var/lib/suricata/update: read/write access

One option is to simply run `suricata-update` as root or with `sudo`.

Note: It is recommended to create a `suricata` group and setup the above directories with the correct permissions for the `suricata` group then add users to the `suricata` group.

Steps to setup the above directories with the correct permissions:

First, create a group `suricata`:

```
sudo groupadd suricata
```

Next, change the group of the directories and its files recursively:

```
sudo chgrp -R suricata /etc/suricata
sudo chgrp -R suricata /var/lib/suricata/rules
sudo chgrp -R suricata /var/lib/suricata/update
```

Note: The paths `/etc/suricata` and `/var/lib` above are used in the default configuration and are dependent on paths set during compilation. By default, these paths are set to `/usr/local`. Please check your configuration for appropriate paths.

Setup the directories with the correct permissions for the `suricata` group:

```
sudo chmod -R g+r /etc/suricata/
sudo chmod -R g+rw /var/lib/suricata/rules
sudo chmod -R g+rw /var/lib/suricata/update
```

Now, add user to the group:

```
sudo usermod -a -G suricata username
```

Verify whether group has been changed:

```
ls -al /etc/suricata
ls -al /var/lib/suricata/rules
ls -al /var/lib/suricata/update
```

Reboot your system. Run `suricata-update` without a sudo to check if suricata-update functions.

1.3 Update Your Rules

Without doing any configuration the default operation of `suricata-update` is to use the Emerging Threats Open ruleset.

Example:

```
suricata-update
```

This command will:

- Look for the `suricata` program on your path to determine its version.
- Look for /etc/suricata/enable.conf, /etc/suricata/disable.conf, /etc/suricata/drop.conf, and /etc/suricata/modify.conf to look for filters to apply to the downloaded rules. These files are optional and do not need to exist.
- Download the Emerging Threats Open ruleset for your version of Suricata, defaulting to 6.0.0 if not found.
- Apply enable, disable, drop and modify filters as loaded above.
- Write out the rules to `/var/lib/suricata/rules/suricata.rules`.
- Run Suricata in test mode on `/var/lib/suricata/rules/suricata.rules`.

Note: Suricata-Update is also capable of triggering a rule reload, but doing so requires some extra configuration that will be covered later. See the documentation of **`--reload-command=<command>`** for more details.

1.4 Configure Suricata to Load Suricata-Update Managed Rules

Note: If `suricata-update` was installed for you by Suricata, then your Suricata configuration should already be setup to work with Suricata-Update.

If upgrading from an older version of Suricata, or running a development version that may not be bundled with Suricata-Update, you will have to check that your `suricata.yaml` is configured for Suricata-Update. The main difference is the `default-rule-path` which is `/var/lib/suricata/rules` when using Suricata-Update.

You will want to update your `suricata.yaml` to have the following:

```
default-rule-path: /var/lib/suricata/rules
rule-files:
  - suricata.rules
```

If you have local rules you would like Suricata to load, these can be listed here as well by using the full path name.

1.5 Discover Other Available Rule Sources

First update the rule source index with the `update-sources` command, for example:

```
suricata-update update-sources
```

Then list the sources from the index. Example:

```
suricata-update list-sources
```

Now enable the **ptresearch/attackdetection** ruleset:

```
suricata-update enable-source ptresearch/attackdetection
```

And update your rules again:

```
suricata-update
```

1.6 List Enabled Sources

```
suricata-update list-sources --enabled
```

1.7 Disable a Source

```
suricata-update disable-source et/pro
```

Disabling a source keeps the source configuration but disables. This is useful when a source requires parameters such as a code that you don't want to lose, which would happen if you removed a source.

Enabling a disabled source re-enables without prompting for user inputs.

1.8 Remove a Source

```
suricata-update remove-source et/pro
```

This removes the local configuration for this source. Re-enabling **et/pro** will requiring re-entering your access code.

CHAPTER

TWO

SURICATA-UPDATE - UPDATE

2.1 Synopsis

`suricata-update` [OPTIONS]

2.2 Description

`suricata-update` aims to be a simple to use rule download and management tool for Suricata.

2.3 Options

-h, **--help**
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, **--quiet**
: Run quietly. Only warning and error messages will be displayed.

-v, **--verbose**
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>
: Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>
: Set a custom user agent string for HTTP requests.

-s, --show-advanced
: Show advanced options.

-o, --output
: The directory to output the rules to.

  Default: */var/lib/suricata/rules*

--force
: Force remote rule files to be downloaded if they otherwise wouldn't be due to just recently downloaded, or the remote checksum matching the cached copy.

--no-merge
: Do not merge the rules into a single rule file.

  Warning: No attempt is made to resolve conflicts if 2 input rule files have the same name.

--yaml-fragment=<filename.yaml>
: Output a fragment of YAML containing the *rule-files* section will all downloaded rule files listed for inclusion in your *suricata.yaml*.

--url=<url>
: A URL to download rules from. This option can be used multiple times.

--local=<filename or directory>
: A path to a filename or directory of local rule files to include.

  If the path is a directory all files ending in *.rules* will be loaded.

  Wildcards are accepted but to avoid shell expansion the argument must be quoted, for example:

  ```
  --local '/etc/suricata/custom-*.rules'
  ```

  This option can be specified multiple times.

--sid-msg-map=<filename>
: Output a v1 style sid-msg.map file.

--sid-msg-map-2=<filename>
: Output a v2 style sid-msg.map file.

--disable-conf=<disable.conf>
: Specify the configuration file for disable filters.

  See *Example Configuration to Disable Rules (–disable-conf)*

--enable-conf=<enable.conf>
: Specify the configuration file for enable rules.

  See *Example Configuration to Enable Rules (–enable-conf)*

--modify-conf=<modify.conf>
: Specify the configuration file for rule modification filters.

  See *Example Configuration to modify Rules (–modify-conf)*

--drop-conf=<drop.conf>

Specify the configuration file for drop filters.

See *Example Configuration to convert Rules to Drop (–drop-conf)*

--ignore=<pattern>

Filenames to ignore. This is a pattern that will be matched against the basename of a rule files.

This argument may be specified multiple times.

Default: **deleted.rules*

Example:

```
--ignore dnp3-events.rules --ignore deleted.rules --ignore "modbus*"
```

Note: If specified the default value of **deleted.rules* will no longer be used, so add it as an extra ignore if needed.

--no-ignore

Disable the –ignore option. Most useful to disable the default ignore pattern without adding others.

--etopen

Download the ET/Open ruleset.

This is the default action of no `--url` options are provided or no sources are configured.

Use this option to enable the ET/Open ruleset in addition to any URLs provided on the command line or sources provided in the configuration.

--dump-sample-configs

Output sample configuration files for the `--disable`, `--enable`, `--modify` and `--threshold-in` commands.

--threshold-in=<threshold.conf.in>

Specify the threshold.conf input template.

--threshold-out=<threshold.conf>

Specify the name of the processed threshold.conf to output.

-T <command>, **--test-command** <command>

Specifies a custom test command to test the rules before reloading Suricata. This overrides the default command and can also be specified in the configuration file under `test-command`.

--no-test

Disables the test command and proceed as if it had passed.

--reload-command=<command>

A command to run after the rules have been updated; will not run if no change to the output files was made. For example:

```
--reload-command='sudo kill -USR2 $(pidof suricata)'
```

will tell Suricata to reload its rules.

Furthermore the reload can be triggered using the Unix socket of Suricata.

Blocking reload (with Suricata waiting for the reload to finish):

```
--reload-command='sudo suricatasc -c reload-rules'
```

Non blocking reload (without restarting Suricata):

```
--reload-command='sudo suricatasc -c ruleset-reload-nonblocking'
```

See the Suricata documentation on Rule Reloads for more information.

--no-reload

Disable Suricata rule reload.

-V, --version

Display the version of **suricata-update**.

--offline

Run offline using most recent cached rules.

2.4 Rule Matching

Matching rules for disabling, enabling, converting to drop or modification can be done with the following:

- signature ID
- regular expression
- rule group
- filename

2.4.1 Signature ID Matching

A signature ID can be matched by just its signature ID, for example:

```
1034
```

The generator ID can also be used for compatibility with other tools:

```
1:1034
```

2.4.2 Regular Expression Matching

Regular expression matching will match a regular expression over the complete rule. Example:

```
re:heartbleed
re:MS(0[7-9]|10)-\d+
```

2.4.3 Group Matching

The group matcher matches against the group the rule was loaded from. Basically this is the filename without the leading path or file extension. Example:

```
group:emerging-icmp.rules
group:emerging-dos
```

Wild card matching similar to wildcards used in a Unix shell can also be used:

```
group:*deleted*
```

2.4.4 Filename Matching

The filename matcher matches against the filename the rule was loaded from taking into consideration the full path. Shell wildcard patterns are allowed:

```
filename:rules/*deleted*
filename:*/emerging-dos.rules
```

2.4.5 Metadata Matching

Rules can be enabled or disabled based on the metadata fields contained in the rule, for example:

```
metadata: deployment perimeter
```

Will match rules that have a metadata field of "deployment" with the value of "perimeter" (case insensitive). This will match on a rule with the provided metadata:

```
metadata:affected_product Any, attack_target Any, deployment Perimeter
```

Note: Metadata matching can only be used to enable, disable or convert rules to drop. It is not available for rule modification.

2.4.6 Modifying Rules

Rule modification can be done with regular expression search and replace. The basic format for a rule modification specifier is:

```
<match> <from> <to>
```

where <match> is one of the rule matchers from above, <from> is the text to be replaced and <to> is the replacement text.

Example converting all alert rules to drop:

```
re:. ^alert drop
```

Example converting all drop rules with noalert back to alert:

```
re:. "^drop(.*)noalert(.*)" "alert\\1noalert\\2"
```

2.5 Order of application of configuration files

1. disable.conf
2. enable.conf
3. drop.conf
4. modify.conf

2.6 Example Configuration Files

2.6.1 Example Configuration File (/etc/suricata/update.yaml)

```
# Configuration with disable filters.
# - Overrided by --disable-conf
# - Default: /etc/suricata/disable.conf
disable-conf: /etc/suricata/disable.conf

# Configuration with enable filters.
# - Overrided by --enable-conf
# - Default: /etc/suricata/enable.conf
enable-conf: /etc/suricata/enable.conf

# Configuration with drop filters.
# - Overrided by --drop-conf
# - Default: /etc/suricata/drop.conf
drop-conf: /etc/suricata/drop.conf

# Configuration with modify filters.
# - Overrided by --modify-conf
# - Default: /etc/suricata/modify.conf
modify-conf: /etc/suricata/modify.conf

# List of files to ignore. Overrided by the --ignore command line option.
ignore:
  - "*deleted.rules"

# Override the user-agent string.
#user-agent: "Suricata-Update"

# Provide an alternate command to the default test command.
#
# The following environment variables can be used.
# SURICATA_PATH - The path to the discovered suricata program.
# OUTPUT_DIR - The directory the rules are written to.
# OUTPUT_FILENAME - The name of the rule file. Will be empty if the rules
#                   were not merged.
```

(continues on next page)

(continued from previous page)

```
#test-command: ${SURICATA_PATH} -T -S ${OUTPUT_FILENAME} -l /tmp

# Provide a command to reload the Suricata rules.
# May be overrided by the --reload-command command line option.
# See the documentation of --reload-command for the different options
# to reload Suricata rules.
#reload-command: sudo systemctl reload suricata

# Remote rule sources. Simply a list of URLs.
sources:
  # Emerging Threats Open with the Suricata version dynamically replaced.
  - https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.tar.gz
  # The SSL blacklist, which is just a standalone rule file.
  - https://sslbl.abuse.ch/blacklist/sslblacklist.rules

# A list of local rule sources. Each entry can be a rule file, a
# directory or a wild card specification.
local:
  # A directory of rules.
  - /etc/suricata/rules
  # A single rule file.
  - /etc/suricata/rules/app-layer-events.rules
  # A wildcard.
  - /etc/suricata/rules/*.rules
```

2.6.2 Example Configuration to Enable Rules (–enable-conf)

```
# suricata-update - enable.conf

# Example of enabling a rule by signature ID (gid is optional).
# 1:2019401
# 2019401

# Example of enabling a rule by regular expression.
# - All regular expression matches are case insensitive.
# re:heartbleed
# re:MS(0[7-9]|10)-\d+

# Examples of enabling a group of rules.
# group:emerging-icmp.rules
# group:emerging-dos
# group:emerging*

# Enable all rules with a metadata of "deployment perimeter". Note that metadata
# matches are case insensitive.
# metadata: deployment perimeter
```

2.6.3 Example Configuration to Disable Rules (–disable-conf)

```
# suricata-update - disable.conf

# Example of disabling a rule by signature ID (gid is optional).
# 1:2019401
# 2019401

# Example of disabling a rule by regular expression.
# - All regular expression matches are case insensitive.
# re:heartbleed
# re:MS(0[7-9]|10)-\d+

# Examples of disabling a group of rules.
# group:emerging-icmp.rules
# group:emerging-dos
# group:emerging*

# Disable all rules with a metadata of "deployment perimeter". Note that metadata
# matches are case insensitive.
# metadata: deployment perimeter
```

2.6.4 Example Configuration to convert Rules to Drop (–drop-conf)

```
# suricata-update - drop.conf
#
# Rules matching specifiers in this file will be converted to drop rules.
#
# Examples:
#
# 1:2019401
# 2019401
#
# re:heartbleed
# re:MS(0[7-9]|10)-\d+
```

2.6.5 Example Configuration to modify Rules (–modify-conf)

```
# suricata-update - modify.conf

# Format: <sid> "<from>" "<to>"

# Example changing the seconds for rule 2019401 to 3600.
# 2019401 "seconds \d+" "seconds 3600"
#
# Example converting all alert rules to drop:
# re:. ^alert drop
#
# Example converting all drop rules with noalert back to alert:
# re:. "^drop(.*)noalert(.*)" "alert\\1noalert\\2"
```

(continues on next page)

(continued from previous page)

```
# Change all trojan-activity rules to drop. Its better to setup a
# drop.conf for this, but this does show the use of back references.
# re:classtype:trojan-activity "(alert)(.*)" "drop\\2"

# For compatibility, most Oinkmaster modifysid lines should work as
# well.
# modifysid * "^drop(.*)noalert(.*)" | "alert${1}noalert${2}"

# Add metadata.
#metadata-add re:"SURICATA STREAM" "evebox-action" "archive"
#metadata-add 2010646 "evebox-action" "archive"
```

CHAPTER

THREE

UPDATE-SOURCES - UPDATE THE SOURCE INDEX

3.1 Synopsis

```
suricata-update update-sources
```

3.2 Description

The `update-sources` command downloads the latest index of available sources.

3.3 Options

-h, **--help**
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, **--quiet**
: Run quietly. Only warning and error messages will be displayed.

-v, **--verbose**
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>
: Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>
: Set a custom user agent string for HTTP requests.

-s, --show-advanced
: Show advanced options.

3.4 Files and Directories

/var/lib/suricata/rules/.cache/index.yaml
: Where the downloaded source index is cached.

3.5 Environment Variables

SOURCE_INDEX_URL
: This environment variable allows the specification of an alternate URL to download the index from.

3.6 URLs

https://www.openinfosecfoundation.org/rules/index.yaml
: The default URL used to download the index from.

CHAPTER

FOUR

LIST-SOURCES - LIST AVAILABLE SOURCES

4.1 Synopsis

```
suricata-update list-sources
```

4.2 Description

The `list-sources` command lists all the available sources.

4.3 Options

-h, **--help**
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, **--quiet**
: Run quietly. Only warning and error messages will be displayed.

-v, **--verbose**
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

--free

List all freely available sources.

--enabled

Lists all the enabled sources.

CHAPTER

FIVE

ENABLE-SOURCE - ENABLE A SOURCE

5.1 Synopsis

```
suricata-update enable-source <source-name> [param=val ...]
```

5.2 Description

Enable a source that is listed in the index.

If the index requires user provided parameters the user will be prompted for them. Alternatively they can be provided on command line to avoid the prompt.

For example:

```
suricata-update enable-source et/pro secret-code=xxxxxxxxxxxxxxx
```

This will prevent the prompt for the et/pro secret code using the value provided on the command line instead.

To update parameters for enabled sources, just re-run the `enable-source` command above again with changed parameters. Changed parameters will be updated in the stored configuration.

5.3 Options

-h, --help
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, --quiet
: Run quietly. Only warning and error messages will be displayed.

-v, --verbose

Provide more verbose output.

--suricata-conf <path>

Path to the suricata config file.

Default: */etc/suricata/suricata.yaml*

--suricata <path>

The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

CHAPTER

SIX

DISABLE-SOURCE - DISABLE AN ENABLED SOURCE

6.1 Synopsis

```
suricata-update disable-source <name>
```

6.2 Description

The `disable-source` command disables a currently enabled source. The configuration for the source is not removed, allowing it to be re-enabled without having to re-enter any required parameters.

6.3 Options

-h, --help
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, --quiet
: Run quietly. Only warning and error messages will be displayed.

-v, --verbose
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

CHAPTER

SEVEN

REMOVE-SOURCE - REMOVE A CONFIGURED SOURCE

7.1 Synopsis

```
suricata-update remove-source <name>
```

7.2 Description

Remove a source configuration. This removes the source file from `/var/lib/suricata/update/sources`, even if its disabled.

7.3 Options

-h, **--help**
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, **--quiet**
: Run quietly. Only warning and error messages will be displayed.

-v, **--verbose**
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

CHAPTER

EIGHT

ADD-SOURCE - ADD A SOURCE BY URL

8.1 Synopsis

```
suricata-update add-source <name> <url>
```

8.2 Description

The `add-source` adds a source to the set of enabled sources by URL. It is useful to add a source that is not provided in the index.

8.3 Options

--http-header "Header: Value"

Add an additional HTTP header to requests for this rule source such as a custom API key. Example:

```
add-source --http-header "X-API-Key: 1234"
```

HTTP basic authentication can be achieved by setting the HTTP Basic Authentication header with `base64(user1:password1)`. Example:

```
add-source --http-header "Authorization: Basic dXNlcjE6cGFzc3dvcmQx"
```

HTTP Bearer authentication can be used by setting the HTTP Bearer Authentication header with a OAuth2 token containing printable ASCII characters. Example:

```
add-source --http-header "Auhorization: Bearer NjA2MTUOTAx?D+wOm4U/vpXQy0xhl!hSaR7
↪#ENVpK59"
```

--no-checksum

Skips downloading the checksum URL for the rule source.

8.4 Common Options

-h, --help

Show help.

-D <directory>, **--data-dir** <directory>

Set an alternate data directory.

Default: */var/lib/suricata*

-c <filename>, **--config** <filename>

Path to the suricata-update config file.

Default: */etc/suricata/update.yaml*

-q, --quiet

Run quietly. Only warning and error messages will be displayed.

-v, --verbose

Provide more verbose output.

--suricata-conf <path>

Path to the suricata config file.

Default: */etc/suricata/suricata.yaml*

--suricata <path>

The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

CHAPTER

NINE

CHECK-VERSIONS - CHECK VERSION OF SURICATA

9.1 Synopsis

```
suricata-update check-versions
```

9.2 Description

The `check-versions` command checks if the installed Suricata version is up to date.

9.3 Options

-h, **--help**
: Show help.

-D <directory>, **--data-dir** <directory>
: Set an alternate data directory.

  Default: */var/lib/suricata*

-c <filename>, **--config** <filename>
: Path to the suricata-update config file.

  Default: */etc/suricata/update.yaml*

-q, **--quiet**
: Run quietly. Only warning and error messages will be displayed.

-v, **--verbose**
: Provide more verbose output.

--suricata-conf <path>
: Path to the suricata config file.

  Default: */etc/suricata/suricata.yaml*

--suricata <path>
: The path to the Suricata program. If not provided `suricata-update` will attempt to find Suricata on your path.

  The Suricata program is used to determine the version of Suricata as well as providing information about the Suricata configuration.

--suricata-version <version>

Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--user-agent <string>

Set a custom user agent string for HTTP requests.

-s, --show-advanced

Show advanced options.

INDEX

Symbols

-D
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
-T
    command line option, 7
-V
    command line option, 8
--config
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
--data-dir
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
--disable-conf
    command line option, 6
--drop-conf
    command line option, 6
--dump-sample-configs
    command line option, 7
--enable-conf
    command line option, 6
--enabled
    command line option, 18
--etopen
    command line option, 7
--force
    command line option, 6
--free
    command line option, 18
--help
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
--http-header
    command line option, 25
--ignore
    command line option, 7
--local
    command line option, 6
--modify-conf
    command line option, 6
--no-checksum
    command line option, 25
--no-ignore
    command line option, 7
--no-merge
    command line option, 6
--no-reload
    command line option, 8
--no-test
    command line option, 7
--offline
    command line option, 8
--output
    command line option, 6
--quiet
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
--reload-command
    command line option, 7
--show-advanced
    command line option, 6, 16, 18, 20, 22, 24, 26, 28
--sid-msg-map
    command line option, 6
--sid-msg-map-2
    command line option, 6
--suricata
    command line option, 5, 15, 17, 20, 21, 23, 26, 27
--suricata-conf
    command line option, 5, 15, 17, 20, 21, 23, 26, 27
--suricata-version
    command line option, 5, 15, 17, 20, 22, 24, 26, 27
--test-command
    command line option, 7
--threshold-in
    command line option, 7
--threshold-out
    command line option, 7
--url
    command line option, 6

--user-agent
    command line option, 6, 16, 18, 20, 22, 24, 26, 28
--verbose
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
--version
    command line option, 8
--yaml-fragment
    command line option, 6
-c
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
-h
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
-o
    command line option, 6
-q
    command line option, 5, 15, 17, 19, 21, 23, 26, 27
-s
    command line option, 6, 16, 18, 20, 22, 24, 26, 28
-v
    command line option, 5, 15, 17, 19, 21, 23, 26, 27

C

command line option
    -D, 5, 15, 17, 19, 21, 23, 26, 27
    -T, 7
    -V, 8
    --config, 5, 15, 17, 19, 21, 23, 26, 27
    --data-dir, 5, 15, 17, 19, 21, 23, 26, 27
    --disable-conf, 6
    --drop-conf, 6
    --dump-sample-configs, 7
    --enable-conf, 6
    --enabled, 18
    --etopen, 7
    --force, 6
    --free, 18
    --help, 5, 15, 17, 19, 21, 23, 26, 27
    --http-header, 25
    --ignore, 7
    --local, 6
    --modify-conf, 6
    --no-checksum, 25
    --no-ignore, 7
    --no-merge, 6
    --no-reload, 8
    --no-test, 7
    --offline, 8
    --output, 6
    --quiet, 5, 15, 17, 19, 21, 23, 26, 27
    --reload-command, 7
    --show-advanced, 6, 16, 18, 20, 22, 24, 26, 28
    --sid-msg-map, 6
    --sid-msg-map-2, 6
    --suricata, 5, 15, 17, 20, 21, 23, 26, 27
    --suricata-conf, 5, 15, 17, 20, 21, 23, 26, 27
    --suricata-version, 5, 15, 17, 20, 22, 24, 26, 27
    --test-command, 7
    --threshold-in, 7
    --threshold-out, 7
    --url, 6
    --user-agent, 6, 16, 18, 20, 22, 24, 26, 28
    --verbose, 5, 15, 17, 19, 21, 23, 26, 27
    --version, 8
    --yaml-fragment, 6
    -c, 5, 15, 17, 19, 21, 23, 26, 27
    -h, 5, 15, 17, 19, 21, 23, 26, 27
    -o, 6
    -q, 5, 15, 17, 19, 21, 23, 26, 27
    -s, 6, 16, 18, 20, 22, 24, 26, 28
    -v, 5, 15, 17, 19, 21, 23, 26, 27